

**Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554**

In the Matter of)	
)	
Advanced Methods to Target and Eliminate)	CG Docket No. 17-59
Unlawful Robocalls)	

COMMENTS OF NEUSTAR, INC.

Neustar, Inc. (“Neustar”) submits these comments in response to the *Public Notice* released on June 20, 2018 in the above-referenced proceeding. The purpose of Neustar’s comments is to provide the Consumer and Governmental Affairs Bureau (“Bureau”) with information that it can use in preparing a staff report on robocalling.

I. Background

Serving as the North American Numbering Plan Administrator, the Thousands-block Pooling Administrator and, until recently, the Local Number Portability Administrator, Neustar has long been recognized for its expertise in telephone numbering issues. In addition to its numbering administration experience, Neustar is also the country’s largest provider of Caller Name (“CNAM”) information for Caller ID displays. Neustar is committed to using its experience with telephone numbering and its involvement with Caller ID to work with the Federal Communications Commission (“FCC”), the Federal Trade Commission (“FTC”), and the telecommunications industry to combat illegal robocalling and Caller ID spoofing.

II. The Call Blocking Order

In the *Public Notice*, the Bureau asks how providers have responded to the permissive rules adopted in the November 2017 *Call Blocking Order*.¹ In addition to incorporating the new rules into the suite of Trusted Call Solutions that Neustar first introduced in the fourth quarter of 2016, discussed in more detail below, Neustar expended considerable effort to educate communications service providers, enterprises, state regulators and state attorneys general about the new rules. Beginning in December 2017 and continuing into February 2018, Neustar conducted a series of three webinars discussing the *Call Blocking Order*. Over 800 people attended at least one of the sessions, a demonstration of the amount of interest the *Call Blocking Order* generated. A copy of the presentation used in one of the webinars is attached.

III. STIR/SHAKEN Deployment

The Bureau also asks about the progress being made toward implementing the STIR/SHAKEN standards for Caller ID authentication. Neustar performs a leading role in the development of the STIR/SHAKEN standards; as a result, it has taken a keen interest in the implementation of STIR/SHAKEN. Since early 2017, Neustar has been the exclusive operator of the ATIS Robocalling Testbed,² with a direct focus on STIR/SHAKEN interoperability testing. Twenty seven participants are formally registered in the Testbed, comprised of a mix of service providers, vendors, and other third party providers of telecommunications services. With recent decisions to move forward with establishing the Secure Telephone Identity Governance Authority (“STI-GA”) and Policy Administrator (“STI-PA”), Neustar has observed a modest increase in both interest in the Testbed and in actual testing. For example, of the ten participants

¹ *Advanced Methods to Target and Eliminate Unlawful Robocalls*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 9706, 9727 (2018) (*Call Blocking Order*).

² <https://www.home.neustar/atis-testbed/index.php>.

completing testing, 60% of this testing was completed in 2018 alone. Testing to date has demonstrated a certain level of industry standards validation, as well as the ability for different implementations to successfully interoperate across interconnecting IP-based networks.

IV. Neustar Trusted Call Solutions

Neustar has introduced a suite of Trusted Call Solutions to help our customers, both service providers and enterprises, to mitigate illegal robocalls. The Trusted Call suite includes the following, which are described in more detail below: Robocall Mitigation, Certified Caller, and Caller Name Optimization/Branded Call Display.

Neustar's Robocall Mitigation solution, unlike most similar services that are targeted to just wireless users, is designed to assist landline customers as well. The solution employs data science and analytics to identify illegal robocallers and then alerts customers via a CNAM overlay – e.g., 'SPAM?_NAME'.³ The solution also incorporates the principles put forward by the Commission in the *Call Blocking Order*. Accordingly, calls that appear to be originating from a telephone number that is unallocated/unassigned, invalid or designated as do-not-originate would receive a CNAM overlay – e.g., 'FRAUDULENT CALL.' Carriers may choose to allow the call to go through with the CNAM overlay alerting customers of the potential danger or may choose to block the call entirely.⁴

Neustar's Certified Caller solution supports the authentication and verification of telephone calls based on the STIR/SHAKEN standards. The solution can be licensed by service providers, vendors and other third-party providers of telecommunications services, and is also

³ See, Press Release, Verizon, SPAM? Verizon gives you a new tool to avoid those pesky robocalls with a new Caller ID feature, April 16, 2018, available at <https://www.verizon.com/about/news/block-spam-robocalls-with-verizon-new-tool>. (last visited July 17, 2018.)

⁴ Not all carriers have the ability to block incoming calls. Alerting consumers to illegal robocalls through the use of CNAM offers an effective tool to protect consumers from harm for those carriers that cannot, or choose not to, block calls.

available as a managed service. Neustar further anticipates offering an extension to its Certified Caller solution that will accelerate the adoption of call authentication where end-to-end Voice over IP (VoIP) is not yet supported.

Neustar's Caller Name Optimization/Branded Call Display allows legitimate businesses to manage their display to consumers (e.g., Name, Logo, Call Purpose). The product incorporates an online portal that allows legitimate businesses to register valid outbound and inbound only (do-not originate) telephone numbers. Neustar utilizes its centralized position in the CNAM ecosystem to distribute both legitimate and do-not-originate telephone number data to the communications ecosystem.

V. Conclusion

Neustar responded to the Commission's *Call Blocking Order* by educating service providers, regulators and enterprises about the new rules and incorporated those new rules into its suite of Trusted Call Solutions. Neustar also continues to work closely with the communications industry on the implementation of the STIR/SHAKEN call authentication standard and supports that standard with the services it offers as part of its Trusted Call Solutions suite. Neustar looks forward to continuing to work with the Commission and the communications industry to combat illegal robocalling.

July 20, 2018

Respectfully submitted,

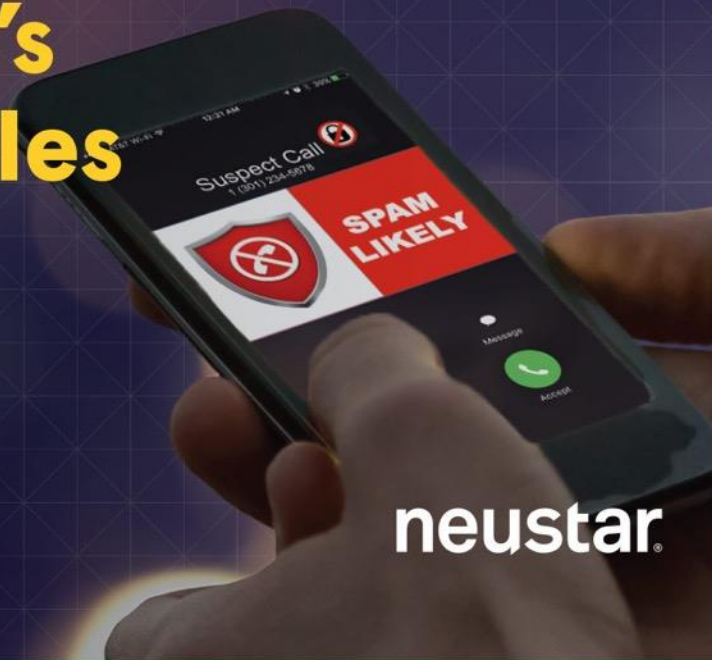
By: /s/ Richard L. Fruchterman, III
Richard L. Fruchterman, III
NEUSTAR, INC.
21575 Ridgetop Circle
Sterling, VA 20166

WEBINAR

What You Need to Know About the FCC's New Call Blocking Rules

Eradicating Robocalls with Regulations, Standards & Solutions

TUESDAY, JANUARY 30, 2018 - 1PM ET/10AM PT



neustar®



Introduction & Overview

Jonjie Sena



Forrester: "Trust is now business currency."

Police warning over scam callers who ask 'Can you hear me?'

Fraud Alert: Watch Out For These Tax-Season Scams

TELEPHONE SCAMS A DAILY OCCURRENCE, POLICE SAY

Credit Card Phone Scam Warning Issued by State Police

Woman defrauded over \$35,000 by callers pretending to be bank officials

Phone Scams Continue to be a Serious Threat, Remain on IRS "Dirty Dozen" List of Tax Scams for the 2016 Filing Season

Department of Financial Regulation: Fake Survey Scam Call

2.9B

US Robocalls per month

Top consumer complaint to FTC, with 5.3M complaints in 2016

Source: FTC, 2017

10x

Phone calls most abused

FTC fraud complaints identify calls as leading method by which fraudsters contact consumers

Source: FTC, 2016

#1

Phone is preferred channel

Over half of all consumers prefer calls as primary channel

Source: Mary Meeker, Internet Trends 2016

88%

Business calls unanswered

B2C answer rates making phone calls ineffective

Source: Boston Consulting Group, 2017

Ajit Pai, FCC Chairman:






"Illegal robocalls not only ruin dinner but they defraud consumers."

"These calls are very likely to be illegal or fraudulent; there's no legitimate reason for anyone to spoof caller ID to make it seem as if he or she is calling from an unassigned or invalid phone number."

"Make no mistake — this isn't the end of our efforts. We'll need to do more, and we will."



OUTLINE

Section	Speaker / Leader		Timing
Intro & Overview: <ul style="list-style-type: none">• How does robocalling and call spoofing impact consumers and businesses?	Jonjie Sena		0:05
Regulatory Perspective <ul style="list-style-type: none">• What do the new FCC call blocking rules mean for you?	Rich Fruchterman		0:10
Commercially available solutions <ul style="list-style-type: none">• What solutions can be implemented now for better call experiences?	Marybeth Degeorgis		0:10
Call authentication standards <ul style="list-style-type: none">• How is the industry addressing call authentication standards?	Ken Politz		0:10
Q&A	Jonjie, All		0:10



Regulatory Perspective

Rich Fruchterman



ROBOCALLING AND RELATIONSHIP TO SPOOFING

Robocalls are prerecorded telemarketing calls to landline home telephones, and all autodialed or prerecorded calls or autodialed text messages to wireless phones. Robocalls can be legitimate or they can be illegitimate (illegal).

Spoofing involves altering the Caller ID information to mask the true origin of a call. Spoofing can also be legitimate or illegitimate (illegal).



Elimination of Illegal Robocalls is one of FCC Chairman Pai's Top Priorities

- Notice of Proposed Rulemaking (NPRM) on Robocall Blocking
- Notice of Inquiry (NOI) on Call Authentication (STIR/SHAKEN) and other methods of identifying illegal robocalls
- NOI on Administration of Call Authentication



REPORT and ORDER on Robocall Blocking

On November 16, the FCC adopted rules that allow service providers to block calls purporting to be from telephone numbers that are:

- **Invalid**
- **Unallocated**
- **Allocated but Unassigned**
- **Designated by the subscriber as numbers that Do-Not-Originate (DNO) calls (in-bound only numbers)**

FCC CALL BLOCKING RULES

Previously, blocking calls violated FCC rules

- Blocking calls by service providers had been deemed an “unjust and unreasonable” practice

Order is permissive, not mandatory

- Service providers **now allowed** to block calls coming from numbers that are invalid, unallocated, allocated but unassigned, or DNO
- Service providers **not required** to block

TYPES OF CALLS TO BLOCK

Invalid and Unallocated Numbers

- The North America Numbering Plan Administrator (NANPA) and the Thousands-block Pooling Administrator (PA) provide service providers with the necessary information to identify invalid and unallocated numbers

Allocated but Unassigned Numbers

- FCC noted service provider sensitivity with sharing numbers that are allocated but unassigned.
- Commission said that service providers can block their own allocated and unassigned, and any of another provider that they know for certain to be unassigned.

DNO Numbers

- Commission also noted the difficulty of sharing information about DNO numbers.
- Commission noted that some providers on the Robocalling Strike Force had begun sharing on a limited basis.

Further Notice of Proposed Rulemaking

FCC also adopted FNPRM to address two issues:

- Potential mechanisms to ensure erroneously blocked calls can be unblocked quickly
- Ways to measure effectiveness of robocalling efforts as well as those of the industry
- Comments due **January 23, 2018**
- Reply Comments due **February 22, 2018**

Finally, the Commission made clear:

- Blocking calls **in accordance** with this order will not violate the FCC's call completion rules
- Blocking calls **outside the scope** of this order may violate the call completion rules
- **NO SAFE HARBOR**





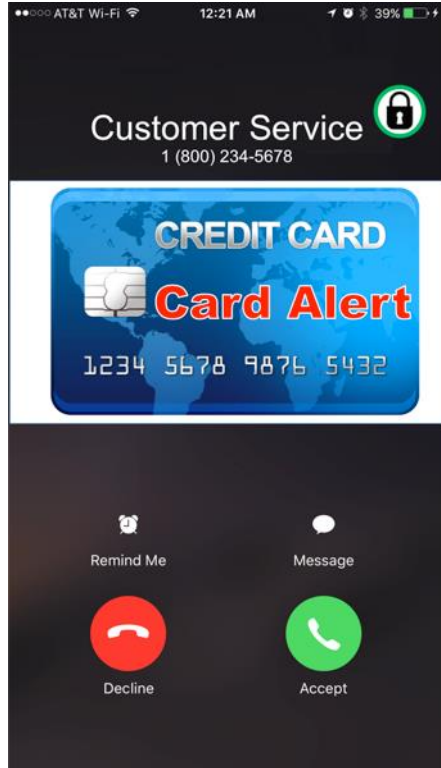
Commercial Solutions

Marybeth Degeorgis



PROTECT SUBSCRIBERS AND IMPROVE CUSTOMER EXPERIENCE

Protect subscribers, stop robocalls, and improve customer engagement



1. Behavioral Analytics, “**Strategic Caller Insights**”

- Detect abnormal or unexpected calling patterns

2. Additional Context, “**Enhanced Caller ID**”

- Full Name, Expanded Name Information
- Business Location, Department
- Logos, E-business cards

3. Call authentication (STIR / SHAKEN), “**Certified Caller ID**”

- Digital certification to fight spoofing & fraud

MOBILE & LANDLINE OPERATORS ARE ROLLING OUT SOLUTIONS TODAY






AT&T Call Protect

More Control over Nuisance Calls






Block that Spam


Prevent annoying inbound calls & email message spam

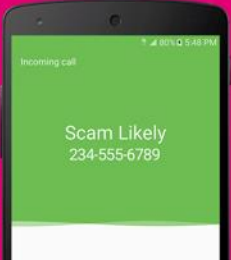
Start Using Spam Controls

It's FREE! Service is limited to Post Pay (monthly) customers.

Already have Spam Controls? [Sign in now.](#)







Scam ID

With Scam ID you'll instantly see when calls come in from known scammers. Only T-Mobile has built this protection right into the network, and it will work automatically on all phones with Caller ID. There's nothing to install and Scam ID is included in all postpaid plans at no additional charge.

verizon



Without Spam Alerts



With Spam Alerts



TODAY, NEUSTAR CAN DELIVER A TRUSTED CALLING EXPERIENCE

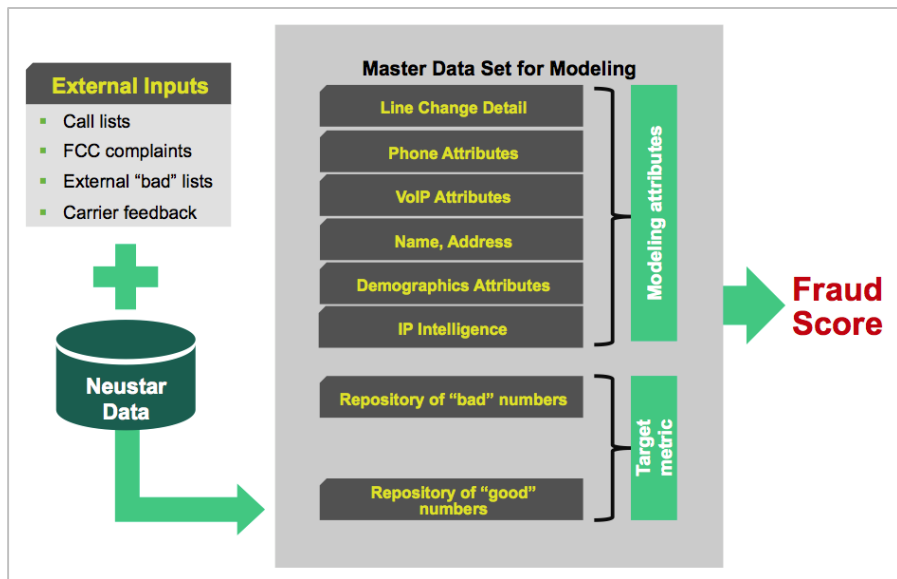
STRATEGIC CALLER INSIGHTS

- Leverages CNAM infrastructure and analytics to detect and warn customers on legacy devices
- Supports *FCC Robocall Blocking* Order (Nov 2017) to *authoritatively identify invalid & unassigned numbers*.
- Policy engine supports operators' customizable business rules for display
- Allows verified enterprises to create *blacklists* of inbound-only, *Do-Not-Originate* numbers
- Allows enterprises to *register verified* outbound numbers to prevent inadvertent blocking or spam-tagging



STRATEGIC CALLER INSIGHTS: NEUSTAR DATA & MODELING TO VERIFY, QUALIFY

Leverage A Broad Range Of
Data Sources To Maximize Value



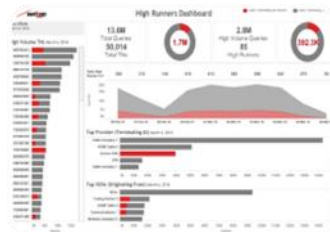
Our Insights & Visualization Identify
Robocalls, Spoofers & Scammers

		Call Volume		
Fraud Score		Low	Med	High
	High	Watch	Analyze	Block
	Med	Low Risk	Watch	Analyze
	Low	Low Risk	Low Risk	Watch

Gain near real-time
access to Neustar's
reliable, proven data

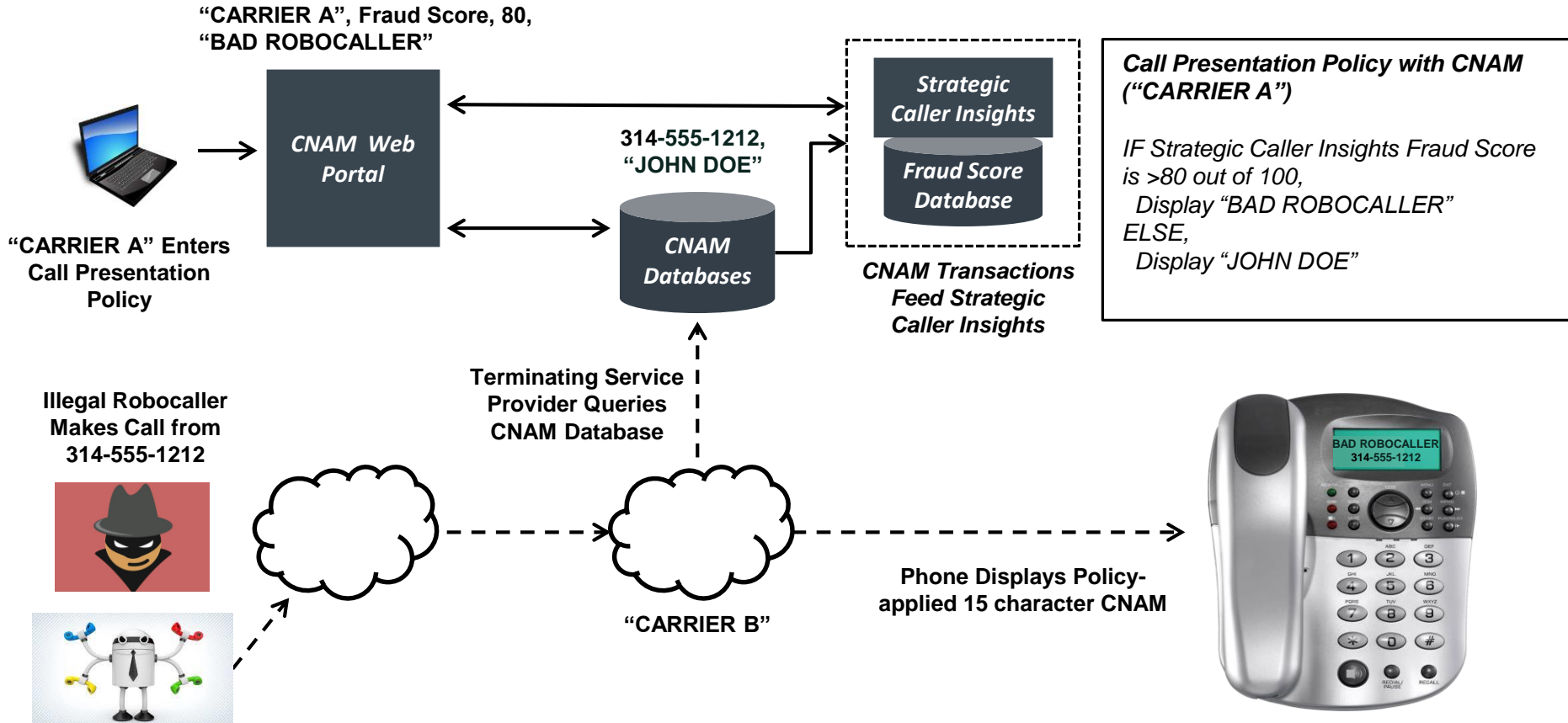


Identify high-volume
robocalls & spoofers
so carriers can
confidently respond



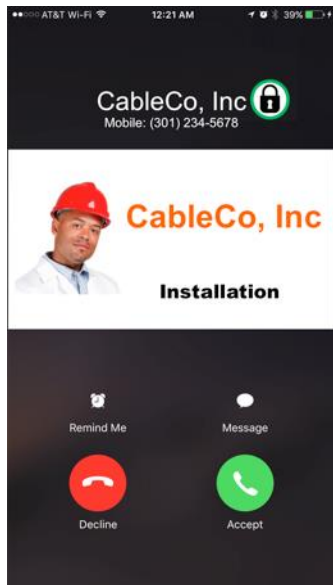
Empower carrier
team to report on
CNAM service
metrics

HOW DOES NEUSTAR ROBOCALLING SOLUTION WORK?



ENHANCED CALLER ID: BRANDED CUSTOMER EXPERIENCE, PERSONALIZED FOR EVERY CONTEXT

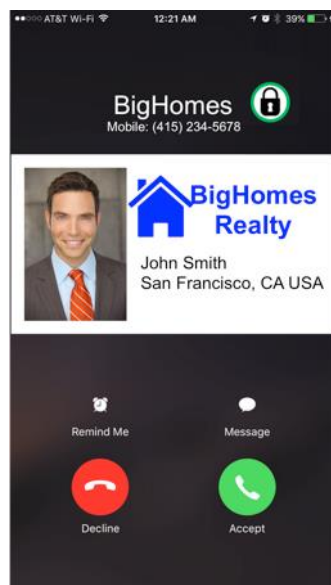
IMPROVE OPERATIONS



Identify your field team

Reach a live customer to reduce truck rolls, gas costs, delivery attempts, and customer frustration.

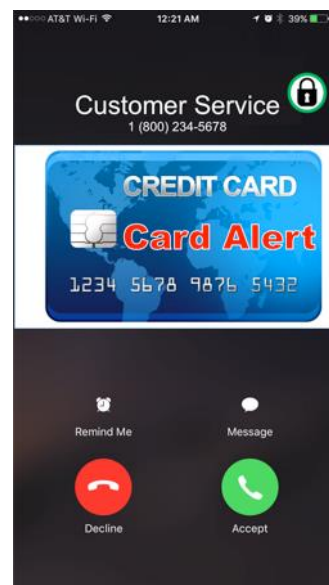
OPTIMIZE ENGAGEMENT



Personalize each call

E-business cards appear with each call or text, so users can identify the caller at a glance, to improve engagement.

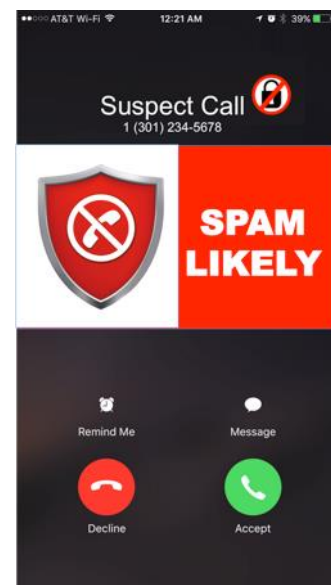
REDUCE RISK



Grab Attention FAST

Establish authenticated context for critical situations. Grab attention to reduce risk & liability for you and your customer.

PROTECT CONSUMERS



Stop Suspicious Callers

Flag suspicious numbers so users can easily block annoying and potentially dangerous callers.

ENHANCE AND MAINTAIN YOUR BRAND IDENTITY ACROSS THE TELECOMMUNICATIONS ECOSYSTEM

1. Strategic Caller Insights

- Protect consumers by notifying them of potential fraudulent calls
- Supports FCC Robocall Blocking Order (Nov 2017) to identify invalid & unassigned numbers.
- Supports verified enterprise blacklist of Do-Not-Originate numbers.
- Supports enterprises to register verified business numbers, to prevent inadvertent blocking or spam-tagging.

2. Enhanced Caller ID for Landline

- Allow enterprises to manage Brand Identity for outbound calls
- Standardize 'Calling Name' 15-character name, or customize per department, geography or function. May be changed on-demand

3. Enhanced Caller ID for Mobile

- Enable personalized mobile branded experiences for phone calls.





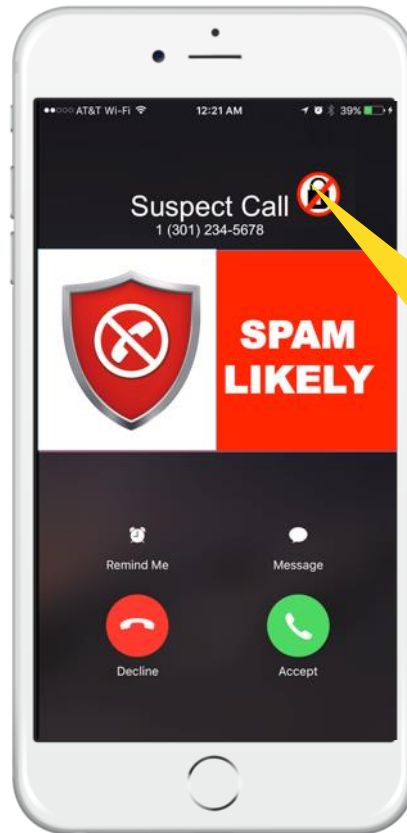
Call Authentication Standards and Industry Testing

Ken Politz

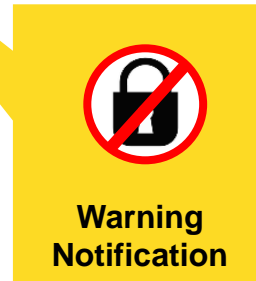


CALL AUTHENTICATION AND CUSTOMER BENEFIT

- Adapt web security techniques to telephone networks
- Initially, originating service provider attests to identity of calling phone number
- Provider digitally signs call and routes signature to its destination
- Terminating service provider verifies digital signature
- Process enhances visual warning / notification to customer, so they can better decide whether to answer



**Caller ID
Override**



CALL AUTHENTICATION BUILT ON CORE INDUSTRY STANDARDS



STIR = Secure Telephone Identity Revisited

- In scope: robocalling, voicemail hacking, swatting, impersonation (spoofing)

Work status (Neustar co-author of each):

- draft-ietf-stir-passport-11 > **RFC 8225**
 - Identity token specification
 - Network protocol independent
- draft-ietf-stir-rfc4474bis-16 > **RFC 8224**
 - SIP token procedures for detecting identity impersonation
- draft-ietf-stir-certificates-18 > **RFC 8226**
 - Credential management systems for supporting call authentication

IP-NNI Task Force (w/SIP Forum)

- Neustar contributed to “Signature based Handling of Asserted information using ToKENs” or SHAKEN; **ATIS-1000074**
- Neustar contributed to “SHAKEN: Governance Model and Certificate Management”; **ATIS-1000080**

Testbeds Focus Group

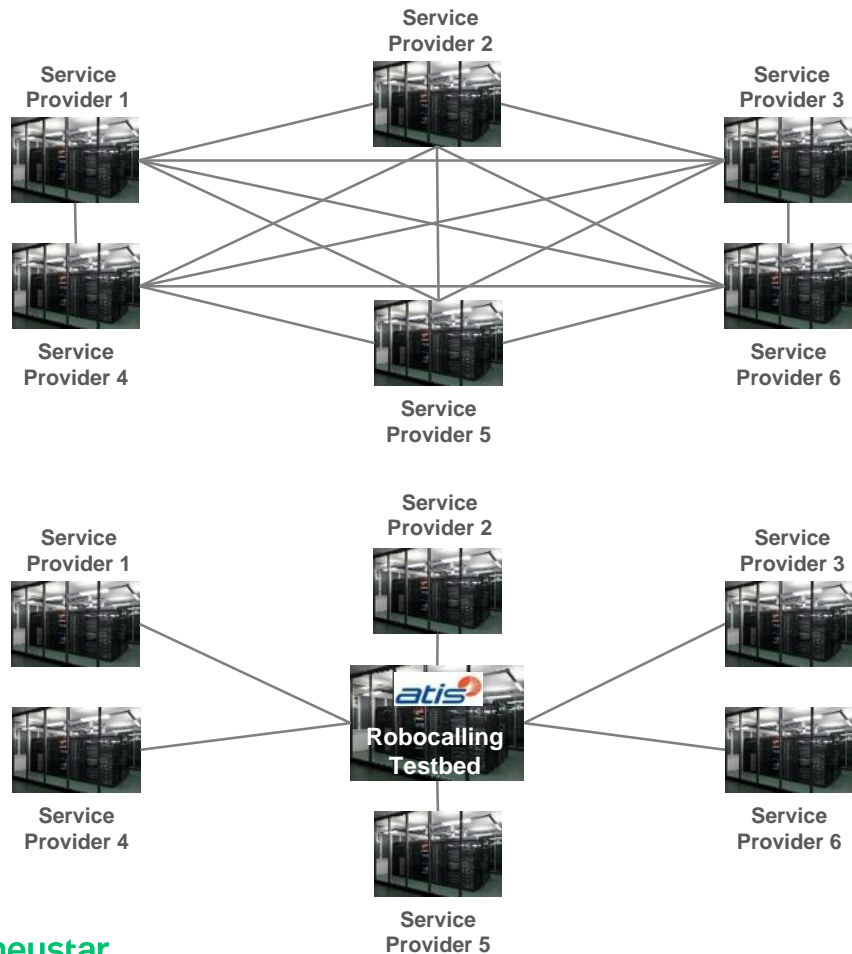
- Neustar contributing to “Secure Telephone Identity (STI) End-to-End Call Test Plan”

ATIS = Alliance for Telecommunications Industry Solutions
IETF = Internet Engineering Task Force

WHAT IS THE ATIS ROBOCALLING TESTBED?

- Virtualized industry test platform to help service providers, suppliers and third parties verify implementations of new SHAKEN call authentication framework
- Established from Robocall Strike Force Report (10/26/2016) and work underway at ATIS Testbeds Focus Group
- Supports testing per applicable ATIS Testbeds Focus Group document(s) and “Authentication” and “Verification” services
- Open to both ATIS members and qualified non-ATIS members
- Testbed hosted & operated by Neustar Trust Lab:
 - Physical lab environment to support remote testing
 - Lab support resources
 - Applicable documentation to support testing
 - Dedicated e-mail for Technical Support requests

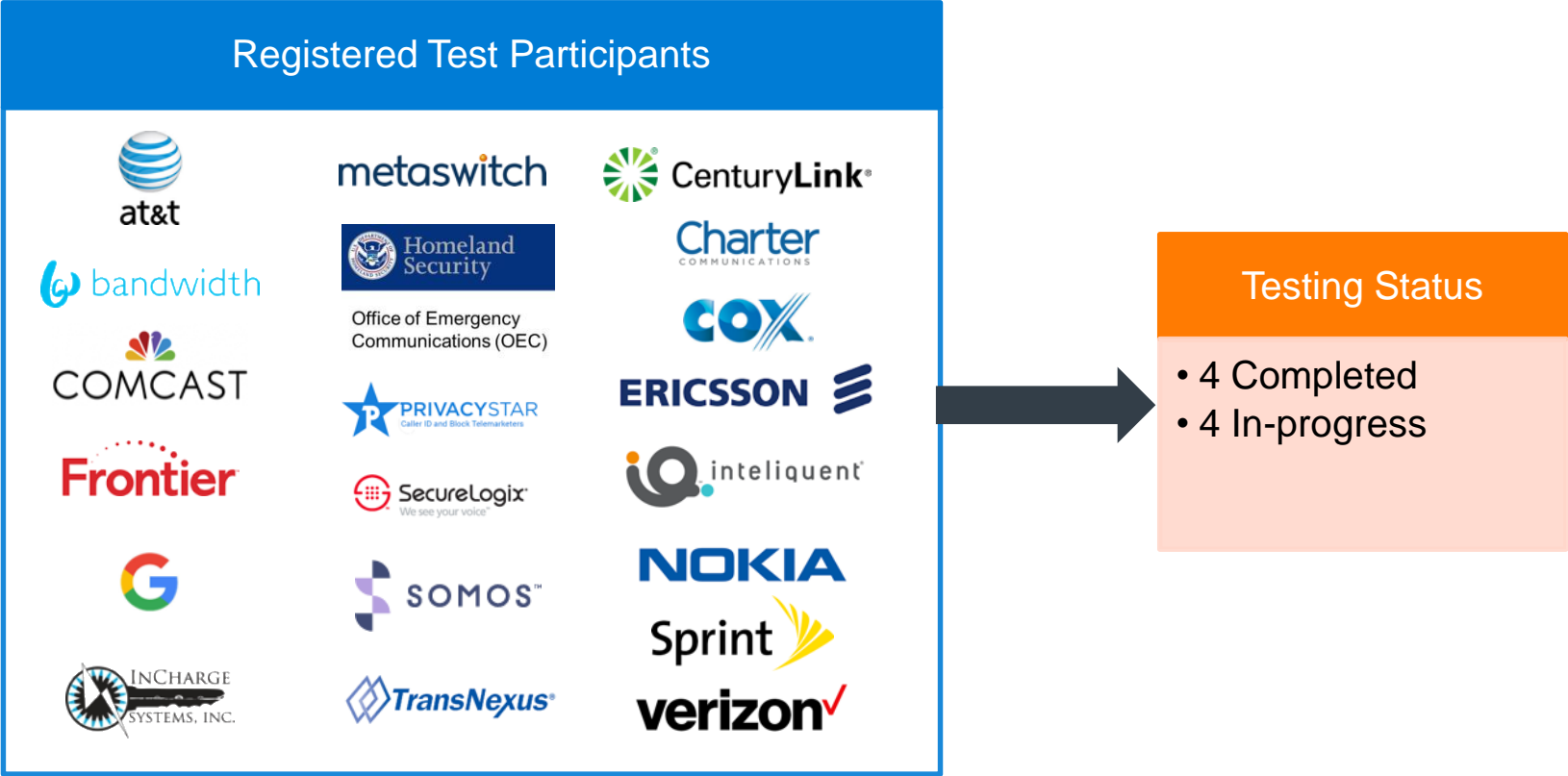
WHY PARTICIPATE IN THE ATIS ROBOCALLING TESTBED?



KEY BENEFITS

1. Test against an emerging “reference” implementation before testing across service provider labs
2. Achieve high level of industry interoperability through ATIS-developed test plans
3. Verify error-handling functionality through automated tool scripts
4. Share/discuss/resolve issues identified during industry testing
5. Leverage uniform set of remote virtual lab access, connectivity and configuration profiles
6. Use Testbed at no cost at least through 1Q 2018

ATIS ROBOCALLING TESTBED TESTING PROGRESSION



ATIS ROBOCALLING TESTBED TESTING TO DATE

- Test cases based on core subset of (living) ATIS Testbeds Focus Group “STI Protocol Test Plan” document
- Address key interoperability areas per published ATIS-1000074 SHAKEN standard
- Experience to date suggests more than one testing session required to complete end-to-end functional testing
- Each collaborative testing session typically lasts about two hours with call traces and results shared in near-real-time to facilitate troubleshooting
- Typical issues encountered:
 - ❑ Setup related – mostly configurations on various elements and firewall rules for access
 - ❑ Error handling – Associated response codes not being generated and relayed back to the originator correctly along with defined reason strings
 - ❑ Implementation – “Identity” header generation software defects
 - ❑ IETF and ATIS standards interpretation
- On completion, Neustar and test participant(s) collaborate on anonymized Test Results Summary

HOW CAN YOU PARTICIPATE IN ATIS ROBOCALLING TESTBED?



ATIS Robocalling Testbed

The ATIS Robocalling Testbed, exclusively hosted by the Neustar Trust Lab, serves as the industry interoperability test facility to validate the effectiveness of caller authentication standards developed by the Internet Engineering Task Force (IETF) and ATIS. Specifically, ATIS developed "Signature-based Handling of Asserted Information using toKENs" (SHAKEN) as an implementation framework for service providers to better combat robocalls and call spoofing on IP-based networks.

The Neustar Trust Lab serves as the virtual industry testbed for communications service providers, equipment manufacturers and software suppliers to remotely test solutions developed for the SHAKEN framework. Participants in the testbed collaborate to test against applicable ATIS standards. Neustar provides technical support for the relevant connectivity information, representative network configuration, its SHAKEN software functionality and supported test scenarios amongst participants. The virtual test environment removes obstacles and accelerates the validation of caller

Registration and Testing Resources

[ATIS Robocalling Testbed Overview](#)

[ATIS Confidentiality Agreement](#)

Download, complete and return via [e-mail](#)

[Neustar Robocalling Testbed Use Policy](#)

Download, complete and return via [e-mail](#)

ATIS Robocalling Testbed Connectivity Guidelines - Participants who have returned both the ATIS Confidentiality Agreement and Neustar Robocalling Testbed Use Policy can request the latest copy by contacting [Technical Support](#).

www.home.neustar/atis-testbed/index.php

Questions?

Slides will be shared after the webinar.



Thank you

Further Questions?

www.callerid.neustar

callerid@team.neustar

+1 (855) 898-0036

